РСТ

ВСЕМИРНАЯ ОРГАНИЗАЦИЯ
ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ
Международное бюро

МЕЖДУНАРОДНАЯ ЗАЯВКА, ОПУБЛИКОВАННАЯ В СООТВЕТСТВИИ С ДОГОВОРОМ О ПАТЕНТНОЙ КООПЕРАЦИИ (РСТ)

(51) Международная классификация изобретения [6]: H04L 9/00	A1	(11) Номер международной публикации: WO 99/44330 (43) Дата международной публикации: 2 сентября 1999 (02.09.99)

(21) Номер международной заявки: PCT/RU98/00181

(22) Дата международной подачи: 19 июня 1998 (19.06.98)

(30) Данные о приоритете:

98103646	24 февраля 1998 (24.02.98)	RU
98104851	20 марта 1998 (20.03.98)	RU
98107784	22 апреля 1998 (22.04.98)	RU

(71) Заявитель *(для всех указанных государств, кроме US)*: ОТКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО МОСКОВСКАЯ ГОРОДСКАЯ ТЕЛЕФОННАЯ СЕТЬ [RU/RU]; 103804 Москва, Дегтярный пер., д. 6, строение 2 (RU) [OTKRYTOE AKTSIONERNOE OBSCHESTVO MOSKOVSKAYA GORODSKAYA TELEFONNAYA SET, Moscow (RU)].

(71)(72) Заявители и изобретатели: МОЛДОВЯН Александр Андреевич [RU/RU]; 188710 Всеволожск, ул. Александровская, д. 88/2, кв. 62 (RU) [MOLDOVYAN, Alexandr Andreevich, Vsevolozhsk (RU)]. МОЛДОВЯН Николай Андреевич [RU/RU]; 188710 Всеволожск, ул. Александровская, д. 88/2, кв. 58 (RU) [MOLDOVYAN, Nikolai Andreevich, Vsevolozhsk (RU)]. САВЛУКОВ Николай Викторович [RU/RU]; 127410 Москва, ул. Инженерная, д. 6, кв. 65 (RU) [SAVLUKOV, Nikolai Viktorovich, Moscow (RU)].

(74) Агент: ООО Центр ИННОТЕК; 105023 Москва, Большая Семёновская ул., д. 49, офис 404 (RU) [OOO TSENTR INNOTEK, Moscow (RU)]

(81) Указанные государства: CN, CZ, JP, KR, PL, SI, SK, UA, US, европейский патент (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Опубликована

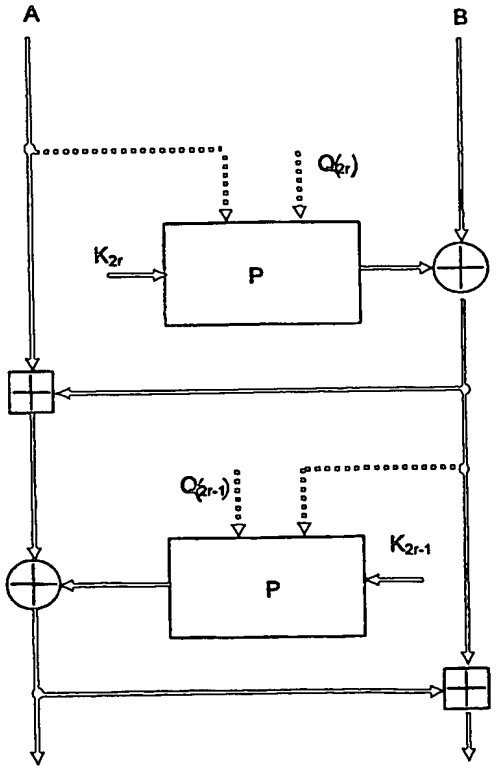
С отчётом о международном поиске.

(54) Title: METHOD FOR THE BLOCK-ENCRYPTION OF DISCRETE DATA

(54) Название изобретения: СПОСОБ БЛОЧНОГО ШИФРОВАНИЯ ДИСКРЕТНЫХ ДАННЫХ

(57) Abstract

The present invention pertains to the field of electrical communications and computer techniques and more precisely relates to cryptographic methods and devices for the encryption digital data. This method comprises forming an encryption key in the shape of a set of sub–keys, breaking down a data block into a number of sub–blocks $N \geq 2$, and successively converting the sub–blocks by carrying out a dual–locus operation on a sub–block and a sub–key. This method is characterised in that before carrying out the dual–locus operation on the i–th sub–block and sub–key, a conversion operation depending on the j–th sub–block is carried out on the sub–key, wherein $j \neq i$. This method is also characterised in thatthe conversion operation depending on the j–th sub–block is a permutation operation on the sub–key bits depending on the j–th sub–block. This method is further characterised in that the conversion operation depending on the j–th sub–block is a cyclic offsetting operation of the sub–key bits depending on the j–th sub–block. This method is finally characterised in that the conversion operation depending on the j–th sub–block is a substitution operation carried out on the sub–key according to the j–th sub–block.



(57) Реферат

Изобретение относится к области электросвязи и вычислительной техники, а конкретнее к области криптографических способов и устройств для шифрования цифровых данных. Способ включает формирование ключа шифрования в виде совокупности подключей, разбиение блока данных на N>2 подблоков и поочередное преобразование подблоков путем выполнения двуместной операции над подблоком и подключом. Новым в заявляемом способе является то, что перед выполнением двуместной операции над i-тым подблоком и подключом над подключом выполняют операцию преобразования, зависящую от j-того подблока, где j≠i. Новым является также то, что в качестве операции преобразования, зависящей от j-того подблока используют операцию перестановки битов подключа, зависящую от j-того подблока. Кроме того новым является то, что в качестве операции преобразования, зависящей от j-того подблока используют операцию циклического сдвига битов подключа, зависящую от j-того подблока. Также новым является то, что в качестве операции преобразования, зависящей от j-того подблока используют операцию подстановки, выполняемую над подключом в зависимости от j-того подблока.

Способ блочного шифрования дискретных данных

Область техники

Изобретение относится к области электросвязи и вычислительной техники, а конкретнее к области криптографических способов и устройств для шифрования сообщений (информации).

Предшествующий уровень техники

В совокупности признаков заявляемого способа используются следующие термины:

-секретный ключ представляет из себя комбинацию битов, известную только законному пользователю;

-ключ шифрования представляет из себя комбинацию битов, используемую при шифровании информационных сигналов данных; ключ шифрования является сменным элементом шифра и используется для преобразования данного сообщения или данной совокупности сообщений; ключ шифрования формируется по детерминированным процедурам по секретному ключу; в ряде шифров в качестве ключа шифрования используется непосредственно секретный ключ;

-шифр представляет собой совокупность элементарных шагов преобразования входных данных с использованием шифрключа; шифр может быть реализован в виде программы для ЭВМ или в виде отдельного электронного устройства;

-подключ представляет собой часть ключа шифрования, используемую на отдельных элементарных шагах шифрования;

-шифрование есть процесс, реализующий некоторый способ преобразования данных с использованием шифрключа, переводящий данные в криптограмму, представляющую собой псевдослучайную последовательность знаков, из которой получение информации без знания ключа шифрования практически невыполнимо;

-дешифрование есть процесс, обратный процедуре шифрования; дешифрование обеспечивает восстановление информации по криптограмме при знании ключа шифрования;

-криптостойкость является мерой надежности защиты

информации и представляет собой трудоемкость, измеренную в количестве элементарных операций, которые необходимо выполнить для восстановления информации по криптограмме при знании алгоритма преобразования, но без знания ключа шифрования.

Известны способы блочного шифрования данных, см. например шифр RC5 [R.Rivest, The RC5 Encryption Algorithm, Fast Software Encryption, Second International Workshop Proceedings (Leuven, Belgium, December 14-16, 1994), Lecture Notes in Computer Science, v. 1008, Springer-Verlag, 1995, pp.86-96]. В известном способе шифрование блоков данных выполняют путем формирования ключа шифрования в виде совокупности подключей, разбиения преобразуемого блока данных на подблоки и поочередного изменения последних с помощью операции циклического сдвига, операции суммирования по модулю 2, выполняемых над двумя подблоками, и операции суммирования по модулю 2^{32}, выполняемых над подблоком и подключом. При этом подключи используются по фиксированному расписанию, т.е. на данном шаге выполнения бинарной операции между подблоком и подключем значение подключа не зависит от входного блока данных. Данный способ блочного шифрования обеспечивает высокую скорость шифрования при реализации в виде программы для ЭВМ.

Однако, данный способ не обладают достаточной стойкостью к дифференциальному и линейному криптоанализу [Kaliski B.S., Yin Y.L. On Differential and Linear Cryptanalysis of the RC5 Encryption Algorithm. Advances in Cryptology - CRYPTO'95 Proc., Springer-Verlag, 1995, pp.171-184.], что связано с тем, что в данном способе на заданных шагах шифрования используются фиксированные подключи для всех возможных входных блоков.

Наиболее близким по своей технической сущности к заявляемому способу блочного шифрования является способ, описанный в стандарте США DES [National Bureau of Standards. Data Encryption Standard. Federal Information Pro-

cessing Standards Publication 46, January 1977]. Данный способ включает в себя формирование ключа шифрования в виде совокупности 48-битовых подключей, разбиении входного блока дискретных данных на два 32-битовых подблока L и R и поочередное преобразование подблоков под управлением секретного ключа. Всего выполняются 16 раундов преобразования 32-битового подблока данных. Каждый раунд преобразования подблока осуществляется путем выполнения следующих процедур: (1) расширения подблока R до 48 бит путем повторения некоторых битов этого подблока: R→R', (2) осуществления операции суммирования по модулю 2 над подблоком и подключом, (3) разбиения подблока R' на восемь 6-битовых подблока, (4) выполнения операции подстановки над каждым 6-битовым подблоком путем замены 6-битовых подблоков на 4-битовые подблоки по известным таблицам подстановки, (5) объединения восьми 4-битовых подблоков в 32-битовый подблок R, (6) осуществления операции перестановки битов подблока R по детерминированному закону, (7) осуществления операции суммирования по модулю 2 подблока R с подблоком L. Каждый раунд завершается перестановкой подблоков R и L. При выполнении текущего раунда шифрования используется фиксированный подключ для всех возможных входных блоков данных. Подключи, используемые при преобразовании подблоков, формируются под управлением 56-битового секретного ключа. Данный способ блочного шифрования информации обладает высокой скоростью преобразований при реализации в виде специализированных электронных схем.

Однако, этот способ имеет недостатки, а именно, он обладает низкой скоростью шифрования при программной реализации. Кроме того, этот способ использует короткий 56-битовый секретный ключ, что позволяет на мощных современных ЭВМ раскрыть секретный ключ методом подбора возможных значений ключа. Это требует выполнения нескольких процедур шифрования, использующих различные секретные ключи, что делает затруднительным получение высокой скорости шиф-

рования даже в случае аппаратной реализации.

В основу изобретения положена задача разработать способ блочного шифрования дискретных данных, в котором преобразование подблоков данных осуществлялось бы таким образом, чтобы обеспечивалось уменьшение числа операций преобразования, приходящихся на один бит входных данных, при одновременном обеспечении высокой криптостойкости, благодаря чему повышается скорость шифрования.

Раскрытие изобретения

Поставленная задача достигается тем, что в способе блочного шифрования дискретных данных, включающем формирование ключа шифрования в виде совокупности подключей, разбиение блока данных на $N \geqslant 2$ подблоков и поочередное преобразование подблоков путем выполнения двуместной операции над подблоком и подключом новым согласно изобретению является то, что перед выполнением двуместной операции над i-тым подблоком и подключом над подключом выполняют операцию преобразования, зависящую от j-того подблока, где $j \neq i$.

Благодаря такому решению структура подключей, используемых на заданном шаге шифрования, зависит от преобразуемых данных и тем самым на данном шаге преобразования для различных входных блоков используются различные модифицированные значения подключей, благодаря чему обеспечивается высокая криптостойкость к дифференциальному криптоанализу при одновременном уменьшении числа раундов шифрования, что и обеспечивает повышение скорости криптографического преобразования.

Новым является также то, что в качестве операции преобразования, зависящей от j-того подблока используют операцию перестановки битов подключа, зависящую от j-того подблока.

Благодаря такому решению обеспечивается повышение скорости шифрования при реализации заявляемого способа в виде электронных устройств шифрования.

Новым является также то, что в качестве операции

преобразования, зависящей от j-того подблока используют операцию циклического сдвига битов подключа, зависящую от j-того подблока.

Благодаря такому решению обеспечивается повышение скорости шифрования при реализации заявляемого способа в виде программ шифрования для ЭВМ.

Кроме того новым является то, что в качестве операции преобразования, зависящей от j-того подблока используют операцию подстановки, выполняемую над подключом в зависимости от j-того подблока.

Благодаря такому решению обеспечивается дополнительное повышение криптостойкости шифрования при одновременном обеспечении высокой скорости шифрования в случае реализации заявляемого способа в виде программ шифрования для ЭВМ.

Ниже сущность заявляемого изобретения более подробно разъясняется примерами его осуществления со ссылками на прилагаемые чертежи.

Краткое описание чертежей

На фиг. 1 представлена обобщенная схема шифрования согласно заявляемому способу.

На фиг. 2 представлена блок-схема элементарного управляемого переключателя, являющегося базовым элементом блока управляемых перестановок. При u=1 входные биты не переставляются, т.е. сигналы на выходе совпадают с сигналами на входе. При u=0 входные биты переставляются.

На фиг. 3 представлена таблица входных и выходных сигналов элементарного управляемого переключателя при высоком потенциале управляющего сигнала.

На фиг. 4 представлена таблица входных и выходных сигналов элементарного управляемого переключателя при низком потенциале управляющего сигнала.

На фиг. 5 схематично представлена структура блока управляемых перестановок, состоящего из совокупности однотипных блоков - элементарных переключателей, реализующей

2^{79} различных перестановок входных битов в зависимости от значения 79-битового управляющего кода.

На фиг. 6 представлена схема упрощенного блока управляемых перестановок.

Лучшие варианты осуществления изобретения

Изобретение поясняется обобщенной схемой криптографического преобразования блоков данных на основе заявляемого способа, которая представлена фиг. 1, где: P - блок управляемой операции, выполняемой над подключом; A и B - преобразуемые n-битовые подблоки; K_{2r}, K_{2r-1} - m-битовые подключи (в общем случае $m \neq n$); Q(2r), Q(2r-1) - g-битовые дополнительные подключи; знак "⊕" обозначает операцию поразрядного суммирования по модулю два, знак "⊞" - операцию суммирования по модулю 2^n. Жирные сплошные линии обозначают шину передачи n-битовых сигналов, тонкие пунктирные линии - передачу одного управляющего бита. Жирные пунктирные линии - шину передачи n управляющих сигналов, в качестве которых используются биты преобразуемых подблоков. Жирные пунктирные линии обозначают также шину передачи h битов дополнительных подключей Q(2r) и Q(2r-1), которые служат для модифицирования операции, зависящей от преобразуемого подблока. В частных случаях дополнительные подключи могут не использоваться.

Фиг. 1 показывает один (r-тый) раунд шифрования. В зависимости от конкретного вида используемой управляемой операции и требуемой скорости преобразований могут быть заданы от 6 до 10 и более раундов. Один раунд преобразования заключается в выполнении следующей последовательности процедур:

(1) преобразование подключа K_{2r} в зависимости от значений подблока A и от значения дополнительного подключа Q(2r), в результате чего на выходе блока P_1 вырабатывается преобразованное значение подключа $P_{A,Q(2r)}(K_{2r})$;

(2) преобразование подблока B путем выполнения операции поразрядного суммирования по модулю 2 над значением $P_{A,Q(2r)}(K_{2r})$ и подблоком B: $B:=B \oplus P_{A,Q(2r)}(K_{2r})$.

где знак ":=" обозначает операцию присваивания;

(3) преобразование подблока A путем выполнения операции суммирования по модулю 2^n над подблоком A и подблоком B: $A:=A \boxplus B$;

(4) преобразование подключа K_{2r-1} в зависимости от значения подблока B и от значения дополнительного подключа Q(2r-1), в результате чего на выходе блока P_2 вырабатывается значение $P_{A,Q(2r-1)}(K_{2r-1})$;

(5) преобразование подблока A:

$A:=A \oplus P_{A,Q(2r-1)}(K_{2r-1})$;

(6) преобразование подблока B: $B:=B \boxplus A$.

В зависимости от конкретного варианта реализации предлагаемого способа блочного шифрования дискретной информации одна и та же пара m-битовых подключей K_2 и K_1 (дополнительных g-битовых подключей Q(2) и Q(1)) может использоваться при выполнении каждого раунда шифрования. Возможен вариант, когда в каждом раунде используются независимые подключи K_{2r} и K_{2r-1} (независимые дополнительные подключи Q(2r) и Q(2r-1)) . Например, при числе раундов r=3 в первом раунде используются подключи K_2 и K_1 (Q(2) и Q(1)), во втором раунде - подключи K_4 и K_3 (Q(4) и Q(3)), в третьем раунде - подключи K_6 и K_5 (Q(6) и Q(5)). Подключи K_{2r}, K_{2r-1} и дополнительные подключи Q(2r), Q(2r-1) могут формироваться по специальным процедурам в зависимости от секретного ключа. Возможен вариант, в котором подключи K_{2r}, K_{2r-1} и дополнительные подключи Q(2r), Q(2r-1) формируются путем генерации по случайному закону.

Возможность технической реализации заявляемого способа поясняется следующими конкретными примерами его осуществления.

Пример 1.

В данном примере поясняется шифрование 64-битовых блоков данных при использовании управляемых перестановок в качестве операции, выполняемой над подключом в зависимости от одного из преобразуемых блоков. Ключ шифрования форми-

руется в виде 16 подключей K_1, K_2, K_3,...K_{16}, каждый из которых имеет длину 32 бит. Дополнительные подключи не используются. Входной блок данных разбивается на два 32-битовых подблока A и B. Шифрование входного блока описывается следующим алгоритмом:

1. Установить счетчик числа раундов:

$$r:=1.$$

2. Преобразовать подблок B в соответствии с выражением:

$$B:=B \oplus P_A(K_{2r}),$$

где $P_A(K_{2r})$ обозначает операцию перестановки битов подключа K_{2r}, выполняемую в зависимости от значения подблока A.

3. Преобразовать подблок A в соответствии с выражением:

$$A:=A \boxplus B.$$

4. Преобразовать подблок A в соответствии с выражением:

$$A:=A \oplus P_B(K_{2r-1}),$$

где $P_B(K_{2r-1})$ обозначает операцию перестановки битов подключа K_{2r-1}, выполняемую в зависимости от значения подблока B.

5. Преобразовать подблок B в соответствии с выражением:

$$B:=B \boxplus A.$$

6. Если $r \neq 8$, то прирастить счетчик $r:=r+1$ и перейти к шагу 2, в противном случае СТОП.

Данный алгоритм ориентирован на реализацию в виде электронных схем. Операции перестановки битов подключа, зависящие от одного из преобразуемых подблоков могут быть выполнены с помощью блока управляемых перестановок, реализованного на основе использования совокупности элементарных переключателей, выполняющих операцию перестановки двух битов.

Фиг. 2 поясняет работу элементарного переключателя, где u - управляющий сигнал, a и b - входные сигналы дан-

ных, c и d - выходные сигналы данных.

Таблицы на фиг. 3 и 4 показывают зависимость выходных сигналов от входных и управляющих сигналов. Из данных таблиц видно, что при u=1 линия a коммутируется с линией c, а линия b - с линией d. При u=0 линия a коммутируется с линией d, а линия b - с линией d. Таким образом, при единичном управляющем сигнале перестановка двух входных битов не осуществляется, а при нулевом управляющем сигнале входные биты переставляются.

На фиг. 5 показана возможная реализация блока управляемых перестановок, использующая совокупность элементарных переключателей S. Данный пример соответствует блоку P с 32-битовым информационным входом и 79-битовым управляющим входом. В качестве информационных сигналов используются биты текущего преобразуемого подключа. В качестве управляющих сигналов используются 32 бита одного из подблоков и 47 битов одного из дополнительных подключей.

Число различных вариантов операции перестановки равно числу возможных кодовых комбинаций на входе управления и составляет 2^{79}, для блока P со структурой, представленной на фиг. 2. Данный блок управляемых перестановок реализует уникальную перестановку входных двоичных разрядов для каждого возможного значения кодовой комбинации на управляющем входе, число которых составляет 2^{79}. Внешние информационные входы блока управляемых перестановок обозначены i1, i2,..., i32, внешние выходы обозначены o1, o2,...,o32 управляющие входы обозначены c1, c2,..., c79. Элементарные переключатели S соединены таким образом, что они образуют матрицу состоящую из 31 строки. В первой строке соединены 31 элементарных переключателей S, во второй строке - 30, в третьей - 29 и т.д. В каждой последующей строке число элементарных переключателей уменьшается на 1. В самой нижней 31-й строке соединен 1 элементарный переключатель.

Строка с номером j≠31 имеет 33-j входов, 33-j выходов и 32-j управляющих входа. Последний (самый правый) вы-

ход j-ой строки является внешним выходом блока управляемых перестановок, оставшиеся 32-j выхода j-строки соединены с соответствующими входами (j+1)-й строки. Последняя 31-я строка имеет два выхода и оба из них являются внешними выходами блока управляемых перестановок. Не более, чем на один управляющий вход каждой строки подается единичный (u=1) управляющий сигнал. Для обеспечения этого требования служат двоично-тридцатидвухричные дешифраторы $F_1, F_2, \ldots, F_{15}$ и двоично-шестнадцатеричный дешифратор F_{16}. Дешифраторы $F_1, F_2, \ldots, F_{15}$ имеют пять внешних управляющих входов, на которые подается произвольный 5-битовый двоичный код, и 32 выхода. Данные дешифраторы вырабатывают только на одном выходе единичный сигнал. На оставшихся 31 выходе устанавливается нулевой сигнал. Дешифратор F_{16} имеет 4 входа, на которые подается произвольный 4-битовый двоичный код, и 16 выходов, из которых только на одном устанавливается единичный сигнал. Для всех дешифраторов $F_1, F_2, \ldots, F_{15}$ и F_{16} каждое входное значение двоичного кода задает единственно возможный номер выхода, на котором устанавливается единичный сигнал (u=1).

Часть выходов дешифратора F_h, где $h \leqslant 15$, соединены с управляющими входами строки с номером h (32-h выходов), а часть выходов - с управляющими входами (32-h)-й строки (h выходов). Таким образом, в каждой строке только на одном элементарном переключателе устанавливается управляющий сигнал u=1. Вход строки, присоединенный к правому входу элементарного переключателя, на который подан единичный управляющий сигнал, коммутируется с внешним выходом блока управляемых перестановок, соответствующим данной строке. Если единичный управляющий сигнал подан на самый левый элементарный переключатель, то с внешним выходом блока управляемых перестановок (блок P) коммутируется самый левый вход строки. Первая строка коммутирует один из внешних входов i1, i2, ..., i32 блока P с внешним выходом o1, а остальные 31 внешних входа - с входами второй строки.

Вторая стока коммутирует один из оставшихся 31 внешнего входа с внешним выходом o2, а оставшиеся 30 внешних входов - с входами 3-ей строки и т.д. Такая структура блока P реализует уникальную перестановку входных битов для каждого значения двоичного кода поданного на 79-битовый управляющий вход блока P.

Возможен следующий вариант использования блока управляемых перестановок P с 32-битовым информационным входом и 79-битовым управляющим входом. В качестве управляющих сигналов, подаваемых на 79-битовый управляющий вход блока управляемых перестановок P, могут использоваться 32 бита подблока A и 47 битов дополнительного 47-битового подключа Q(2r). В этом случае в зависимости от 47-битового дополнительного подключа формируется одна из 2^{47} различных модификаций операции перестановки битов, зависящей от значения входного блока. При этом каждая модификация этой операции включает 2^{32} различных операций перестановки битов подключа K_{2r}, причем выбор конкретной операции перестановки определяется значением подблока A. Выбор модификации не является заранее предопределенным, поскольку он определяется дополнительным подключом Q(2r), который является непосредственно элементом секретного ключа или зависит от секретного ключа. Это дополнительно повышает стойкость криптографического преобразования. Если в устройстве шифрования используются два блока P, имеющих структуру, показанную на фиг. 2, то число возможных комбинаций модификаций управляемой операции перестановок, устанавливаемых на блоках P в зависимости от дополнительных 47-битовых подключей, может быть задано до $(2^{47})^2=2^{94}$ при использовании секретного ключа длиной 94 бит.

Благодаря простой структуре блоков P, современная технология изготовления интегральных схем позволяет легко изготовить криптографические микропроцессоры, содержащие управляемые блоки перестановок с размером входа 32 и 64 бит и обеспечивающие скорость шифрования до 1 Гбит/с и вы-

ше.

На фиг. 6, где тонкие сплошные линии обозначают передачу одного бита подключа, показана возможная реализация блока управляемых перестановок, использующая совокупность элементарных переключателей S. Данный пример блока управляемых перестановок соответствует блоку управляемых перестановок с 8-битовым входом для информационных сигналов (битов подключа) и 8-битовым входом для управляющих сигналов (битов подблока данных, обозначенных пунктирными линиями аналогично обозначению на фиг. 1). Аналогично может быть построен произвольный блок управляемых перестановок, например, имеющий 64-битовый вход для информационных сигналов и 128-битовый вход для управляющих сигналов. При использовании блока управляемых перестановок с 32-битовым информационным входом число различных перестановок равно 2^{32}. Это означает, что при шифровании двух различных блоков данных вероятность повторения некоторой перестановки на заданном шаге равна 2^{-32}, а повторение перестановок на z заданных шагах равна 2^{-32z}. Таким образом, набор модифицированных значений подключей, используемых для преобразования каждого входного сообщения, практически является уникальным, что обеспечивает высокую криптостойкость шифрования.

При использовании упрощенной структуры блока управляемых перестановок, схематично представленой на фиг. 6, легко осуществить изготовление криптографических микропроцессоров, содержащих блоки управляемых перестановок с размером входа до 128 бит. Использование операции управляемых перестановок над 128-битовыми подключами позволяет получить более высокую криптостойкость шифрования. Блок управляемых перестановок представляет собой комбинационную электрическую схему, что обеспечивает высокую скорость выполнения управляемых перестановок.

Пример 2.

Данный пример поясняет использование операции цикли-

ческого сдвига, зависящей от преобразуемых подблоков и выполняемой над подключами. Ключ шифрования формируется в виде 16 подключей K_1, K_2, $K_3, \ldots, K_{32}$, каждый из которых имеет длину 32 бит. Входной 64-битовый блок данных разбивается на два 32-битовых подблока A и B. Шифрование входного блока описывается следующим алгоритмом:

1. Установить счетчик числа раундов r=1.

2. Преобразовать подблок B в соответствии с выражением: $B:=B \oplus (K_{2r}<<<A)$, где $K_{2r}<<<A$ обозначает операцию циклического сдвига влево на A бит, выполняемую над подключом K_{2r}.

3. Преобразовать подблок A в соответствии с выражением:

$$A:=A \boxplus B,$$

где "$\boxplus$" - операция суммирования по модулю 2^{32}.

4. Преобразовать подблок A в соответствии с выражением:

$$A:=A \oplus (K_{2r-1}<<<B),$$

где $K_{2r-1}<<<B$ обозначает операцию циклического сдвига влево на B бит, выполняемую над подключом K_{2r-1}.

5. Преобразовать подблок B в соответствии с выражением:

$$B:=B \boxplus A .$$

6. Если $r \neq 16$, то прирастить счетчик $r:=r+1$ и перейти к шагу 2, в противном случае СТОП.

Схема одного раунда преобразований поясняется на фиг. 1, блоки P_1 и P_2 в данном примере представляют собой операционный блок, выполняющий операцию циклического сдвига битов соответствующих подключей в зависимости от преобразуемых подблоков. Данный алгоритм ориентирован на реализацию в виде программы для ЭВМ. Современные микропроцессоры быстро осуществляют операцию циклического сдвига, в зависимости от значения переменной, хранящейся в одном из регистров. Благодаря этому описанный алгоритм при программной реализации обеспечивает скорость шифрования около

40 Мбит/с для массового микропроцессора Pentium/200. При задании 10 раундов шифрования достигается скорость около 60 Мбит/с.

Пример 3.

Данный пример поясняет использование операции подстановки, зависящей от преобразуемых подблоков и выполняемой над подключами. Для данного примера блоки P_1 и P_2 представляют собой операционный блок, выполняющий операцию подстановки в зависимости от соответствующих подблоков. Под операцией подстановки мы понимаем операцию замены двоичного значения сигнала на входе операционного блока P на другое двоичное значение (устанавливаемое на выходе операционного блока P), которое выбирается в зависимости от значения на входе блока P в соответствии с некоторой таблицей замены. Могут быть реализованы два варианта подстановок:

(1) n-битовый входной двоичный вектор заменяется на n-битовый выходной двоичный вектор, причем различным входным двоичным векторам соответствуют различные выходные двоичные вектора;

(2) m-битовый двоичный вектор заменяется на n-битовый двоичный вектор, где $n \geq m$, причем различным входным двоичным векторам могут соответствовать как различные, так и одинаковые выходные двоичные вектора.

Поясним задание зависимости операции подстановки первого типа от подблока преобразуемых данных . Пусть операции подстановки выполняются над двоичными векторами длиной n бит, где n - целое число. Тогда для определения операции подстановки размера nxn (обозначение nxn означает что входным для операции подстановки является двоичный вектор длиной n бит и выходной двоичный вектор также имеет длину n бит) требуется использование таблицы содержащей две строки чисел:

0	1	2	3	...	N-1
α_0	α_1	α_2	α_3	...	α_{N-1} ,

где $N=2^n$. В данной таблице в нижней строке присутствуют все возможные значения n-битового блока ровно по одному разу, но в произвольном порядке. Очередность расположения чисел в нижней строке определяет конкретный вариант таблицы подстановки, а следовательно и конкретный вариант операции подстановки, выполняемой с использованием этой таблицы. Выполнение операции подстановки осуществляется следующим образом. Выбирается в верхней строке число, которое равно значению входного блока. Находящееся под этим числом значение в нижней строке берется в качестве выходного блока. Таким образом, таблицу подстановки можно разместить в оперативной памяти ЭВМ как последовательную запись n-битовых компьютерных слов, размещенных в ячейках с адресами $W_0, W_1, W_2, \ldots, W_{N-1}$. В этом случае значение входного двоичного вектора Y служит для вычисления адреса w_0+Y слова, которое берется в качестве выходного двоичного вектора. Этот способ представления таблицы подстановки требует использования объема памяти равного $Nn=2^n n$ бит. Выберем количество таблиц подстановки равное 2^L (объем требуемой памяти составит при этом $2^L Nn$ бит) и разместим таблицы подстановок непрерывно друг за другом. В качестве адреса таблицы с номером v возьмем значение адреса w_0 ее первого n-битового слова. Пусть адрес таблицы с номером v=0 есть s. В этом случае адрес таблицы подстановки с любым номером v равен s+vN. Если задан управляющий двоичный вектор определяющий номер текущей таблицы подстановки v и текущий входной двоичный вектор, то операция подстановки выполняется заменой текущего входного блока на n-битовое слово, расположенное по адресу s+vN+Y, где Y - значение входного двоичного вектора, над которым выполняется текущая операция подстановки. Используя это соотношение легко задать выбор таблицы подстановки с номером v и выполнить подстановку над входным двоичным вектором со значением Y. В рассмотренном случае задание зависимости таблиц подстановок от значения управляющего двоичного вектора и выполне-

ние операции подстановки осуществляется микропроцессором очень быстро при выборе соответствующих значений параметров L и n, например при L=5 и n=8. При указанных параметрах для размещения таблиц подстановки требуется 8 Кбайт оперативной памяти, что является приемлемым, поскольку современные ЭВМ обладают объемом оперативной памяти на многие порядки больше этой величины (от 1 до 64 Мбайт и более).

Поясним задание зависимости операции подстановки второго типа от подблока данных на примере подстановок 16x32, задаваемых с помощью пронумерованной последовательности 32-битовых двоичных векторов X_j, $j=0,1,2,\ldots,2^{16}-1$. Последовательность X_j предполагается известной и относящейся к описанию алгоритма шифрования. Операция подстановки над 16-битовым подключом k осуществляется в зависимости от преобразуемого подблока b следующим образом:

(1) вычисляется номер $j=(b+k) \bmod 2^{16}$;

(2) 16-битовый двоичный вектор k заменяется на 32-битовый двоичный вектор X_j.

Шифрование 64-битовых блоков данных на основе операций подстановки, выполняемых с помощью последовательности 32-битовых двоичных векторов X_j ($j=0,1,2,\ldots,2^{16}-1$) над подключами в зависимости от преобразуемых подблоков данных, может быть осуществлено, например, следующим образом. Ключ шифрования формируется в виде 16 подключей K_1, K_2, $K_3,\ldots, K_{32}$, каждый из которых имеет длину 16 бит. Входной блок данных разбивается на два 32-битовых подблока $A=a_2|a_1$ и $B=b_2|b_1$, представленные в виде конкатенации 16-битовых подблоков a_1, a_2 и b_1, b_2, соответственно. Шифрование входного блока описывается следующим алгоритмом:

1. Установить счетчик числа раундов r=1.

2. Преобразовать подблок B в соответствии с выражением:

$$B:=B \oplus F(K_{4r}, a_1),$$

где $F(K_{4r}, a_1)$ обозначает операцию подстановки над под-

ключом K_{4r} зависящую от подблока a_1.

3. Преобразовать подблок A в соответствии с выражением:

$$A:=A + B \pmod{2^{32}}.$$

4. Преобразовать подблок A в соответствии с выражением:

$$A:=A \oplus F(K_{4r-1}, b_1),$$

где $F(K_{4r-1}, b_1)$ обозначает операцию подстановки над подключом K_{4r-1}, выполняемую в зависимости от подблока b_1.

5. Преобразовать подблок B в соответствии с выражением:

$$B:=B + A \pmod{2^{32}}.$$

6. Преобразовать подблок B в соответствии с выражением:

$$B:=B \oplus F(K_{4r-2}, a_2).$$

7. Преобразовать подблок A в соответствии с выражением:

$$A:=A + B \pmod{2^{32}}.$$

8. Преобразовать подблок A в соответствии с выражением:

$$A:=A \oplus F(K_{4r-3}, b_2).$$

9. Преобразовать подблок B в соответствии с выражением:

$$B:=B + A \pmod{2^{32}}.$$

10. Если $r \neq 4$, то прирастить счетчик $r:=r+1$ и перейти к шагу 2, в противном случае СТОП.

Данный алгоритм использует известную таблицу подстановки размером 240 Кбайт, что составляет малую часть объема оперативной памяти современных ЭВМ. Операция извлечения двоичных векторов из оперативной памяти по заданным адресам осуществляется за малое число машинных тактов, благодаря чему программная реализация предлагаемого способа блочного шифрования с операциями подстановки, выполняемыми над подключами в зависимости от преобразуемых подблоков, обеспечивает скорость шифрования от 20 до 60 Мбит/с

(в зависимости от конкретной реализации) для массового микропроцессора Pentium/200.

Промышленная применимость

Приведенные примеры показывают, что предлагаемый способ блочного шифрования дискретных данных технически реализуем и позволяет решить поставленную задачу.

Рассмотренные примеры легко реализуемы, например, в специализированных микроэлектронных схемах шифрования (пример 1) и в виде программ шифрования для ЭВМ (примеры 2 и 3) и обеспечивают скорость шифрования до 1 Гбит/с и выше (пример 1) при аппаратной реализации и до 60 Мбит/с при программной реализации и использовании массового микропроцессора Pentium/200 (примеры 2 и 3).

Формула изобретения

1. Способ блочного шифрования дискретных данных, включающий формирование ключа шифрования в виде совокупности подключей, разбиение блока данных на $N \geq 2$ подблоков и поочередное преобразование подблоков путем выполнения двуместной операции над подблоком и подключом, о т л и ч а ю щ и й с я тем, что перед выполнением двуместной операции над i-тым подблоком и подключом над подключом выполняют операцию преобразования, зависящую от j-того подблока, где $j \neq i$.

2. Способ по п.1, о т л и ч а ю щ и й с я тем, что что в качестве операции преобразования, зависящей от j-того подблока используют операцию перестановки битов подключа, зависящую от j-того подблока.

3. Способ по п.1, о т л и ч а ю щ и й с я тем, что в качестве операции преобразования, зависящей от j-того подблока используют операцию циклического сдвига битов подключа, зависящую от j-того подблока.

4. Способ по п.1, о т л и ч а ю щ и й с я тем, что в качестве операции преобразования, зависящей от j-того подблока используют операцию подстановки, выполняемую над подключом в зависимости от j-того подблока.

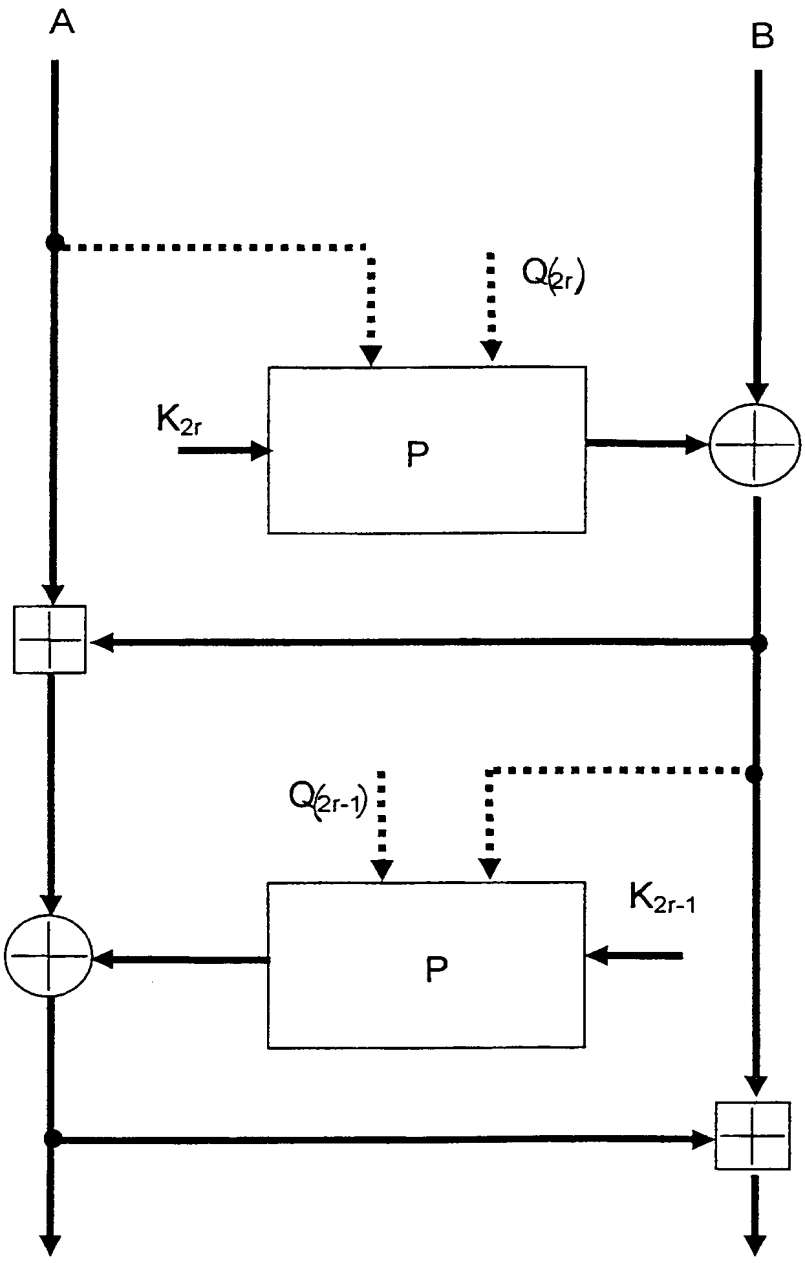


Fig.1.

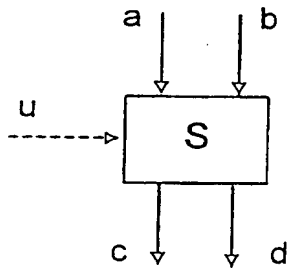


Fig.2.

u=1

INPUT		OUTPUT	
a	b	c	d
1	0	1	0
0	1	0	1
0	0	0	0
1	1	1	1

Fig.3.

u=0

INPUT		OUTPUT	
a	b	c	d
0	1	1	0
1	0	0	1
0	0	0	0
1	1	1	1

Fig.4.

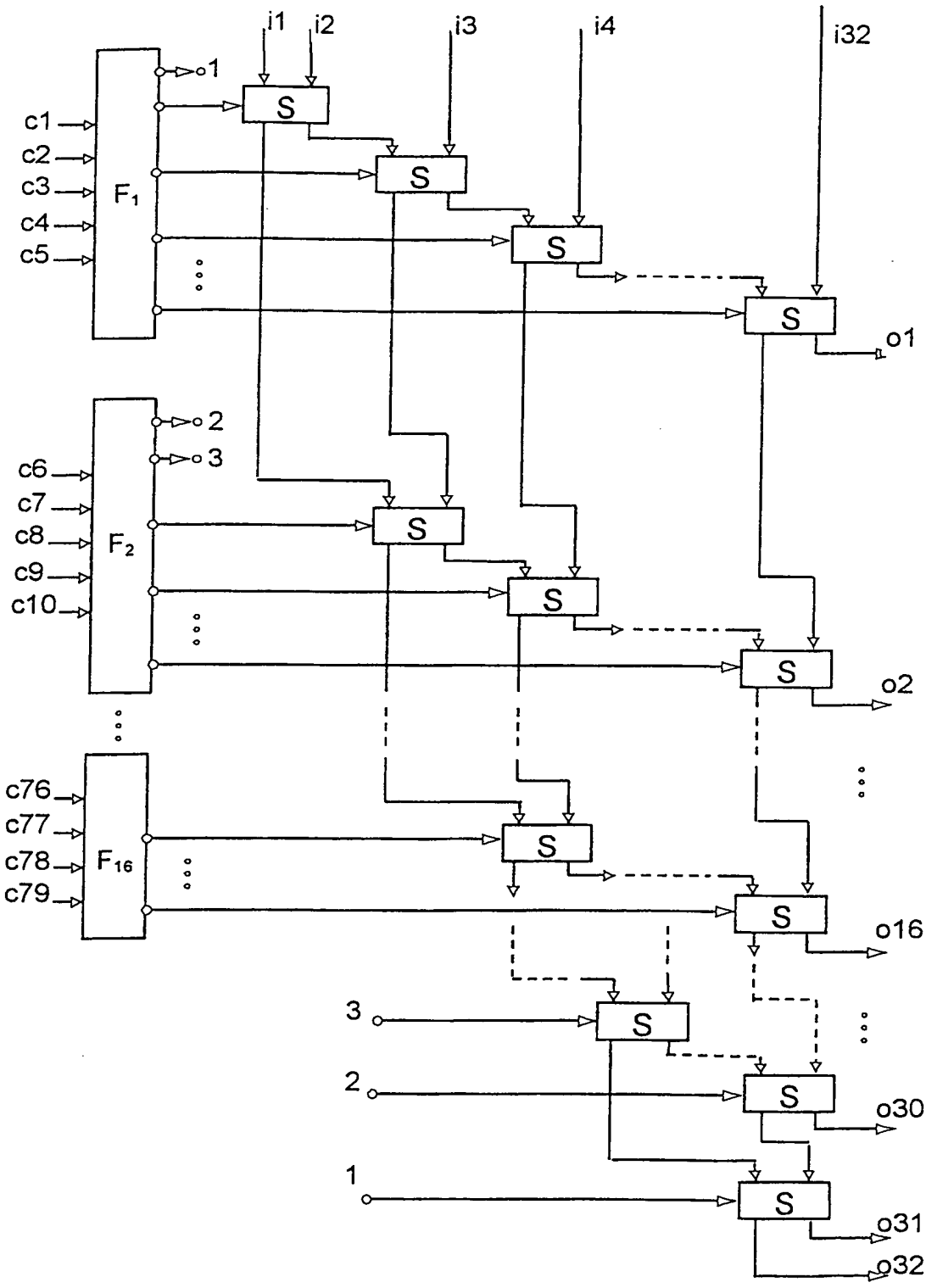

i1
i2
i3
i4
i32
o1
c1
c2
c3
c4
c5
F1
S
o2
c6
c7
c8
c9
c10
F2
o16
c76
c77
c78
c79
F16
3
2
1
o30
o31
o32

Fig. 5.

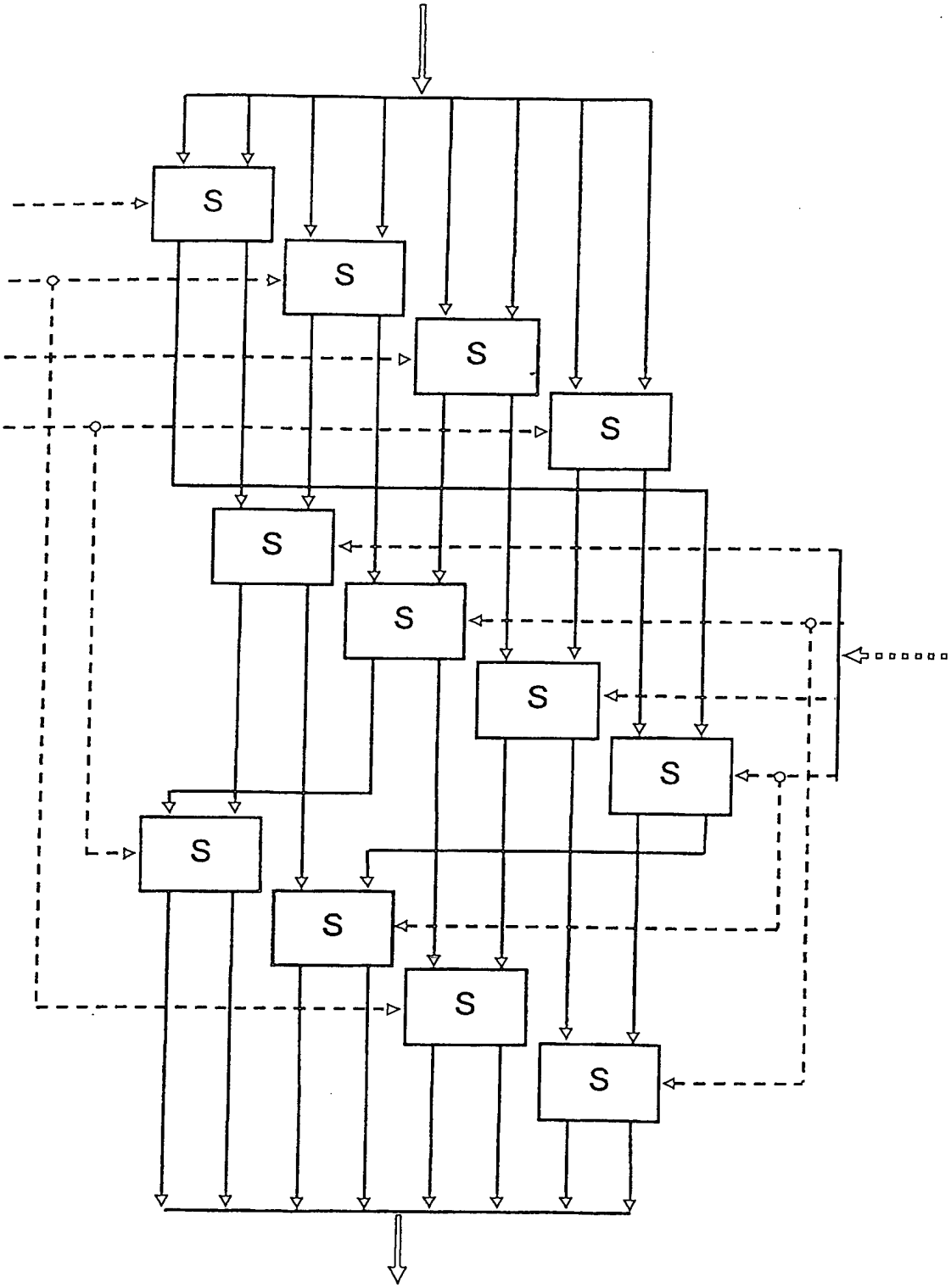


Fig.6.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/RU 98/00181

A. CLASSIFICATION OF SUBJECT MATTER [6]:
IPC6 H04L 9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC6 H04L 9/00, H04L 9/08, H04L 9/14, H04L 9/28, H04K 1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	RU 2103828 C1 (UPRAVLENIE FEDERALNOI SLUZHBY BEZOPASNOSTI ROSII PO SANKT PETERBURGU I LENINGRAOSKOI OBLASTI et al.) 27 January 1998 (27.01.98)	1-4
A	EP 0173647 A2 (GRETAG AKTIENGESELLSCHAFT) 05 March 1986 (05.03.86)	1-4
A	WO 97/12459 A1 (LIN, Xiankan) 03 April 1997 (03.04.97)	1-4
A	US 5548648 A (INTERNATIONAL BUSINESS MACHINES Corp.) 20 August 1996 (20.08.96)	1-4

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 September 1998 (18.09.98)	28 October 1998 (28.10.98)
Name and mailing address of the ISA/ RU Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

ОТЧЕТ О МЕЖДУНАРОДНОМ ПОИСКЕ

Международная заявка № PCT/RU 98/00181

A. КЛАССИФИКАЦИЯ ПРЕДМЕТА ИЗОБРЕТЕНИЯ:

H04L 9/00

Согласно международной патентной классификации (МПК-6)

B. ОБЛАСТИ ПОИСКА:

Проверенный минимум документации (система классификации и индексы) МПК-6:

H04L 9/00, H04L 9/08, H04L 9/14, H04L 9/28, H04K 1/00

Другая проверенная документация в той мере, в какой она включена в поисковые подборки:

Электронная база данных, использовавшаяся при поиске (название базы и, если возможно, поисковые термины):

C. ДОКУМЕНТЫ, СЧИТАЮЩИЕСЯ РЕЛЕВАНТНЫМИ

Категория*	Ссылки на документы с указанием, где это возможно, релевантных частей	Относится к пункту №
A	RU 2103828 C1 (УПРАВЛЕНИЕ ФЕДЕРАЛЬНОЙ СЛУЖБЫ БЕЗОПАСНОСТИ РОССИИ ПО САНКТ-ПЕТЕРБУРГУ И ЛЕНИНГРАДСКОЙ ОБЛАСТИ и др.) 27.01.98	1 - 4
A	EP 0173647 A2 (GRETAG AKTIENGESELLSCHAFT) 05.03.86	1 - 4
A	WO 97/12459 A1 (LIN, Xiankan) 03.04.97	1 - 4
A	US 5548648 A (INTERNATIONAL BUSINESS MACHINES Corp.) Aug. 20, 1996	1 - 4

☐ последующие документы указаны в продолжении графы C.

☐ данные о патентах-аналогах указаны в приложении

* Особые категории ссылочных документов:

"A" документ, определяющий общий уровень техники

"E" более ранний документ, но опубликованный на дату международной подачи или после нее

"O" документ, относящийся к устному раскрытию, экспонированию и т.д.

"P" документ, опубликованный до даты международной подачи, но после даты испрашиваемого приоритета

"T" более поздний документ, опубликованный после даты приоритета и приведенный для понимания иззобретения

"X" документ, имеющий наиболее близкое отношение к предмету поиска, порочащий новизну и изобретательский уровень

"Y" документ, порочащий изобретательский уровень в сочетании с одним или несколькими документами той же категории

"&" документ, являющийся патентом-аналогом

Дата действительного завершения международного поиска: 18 сентября 1998 (18.09.98)

Дата отправки настоящего отчета о международном поиске: 28 октября 1998 (28.10.98)

Наименование и адрес Международного поискового органа:

Федеральный институт промышленной собственности

Россия, 121858, Москва, Бережковская наб., 30-1

Факс: 243-3337, телетайп: 114818 ПОДАЧА

Уполномоченное лицо:

Д.Смирнов

Телефон №: (095)240-5888

Форма PCT/ISA/210 (второй лист) (июль 1992)